COUNTING SCHUR RINGS OVER CYCLIC GROUPS

ANDREW MISSELDINE

Abstract. Any Schur ring is uniquely determined by a partition of the elements of the group. An open question in the study of Schur rings is determining which partitions of the group induce a Schur ring. Although a structure theorem is available for Schur rings over cyclic groups, it is still a difficult problem to count all the partitions. For example, Kovacs, Liskovets, and Poschel determine formulas to count the number of wreath-indecomposable Schur rings. In this paper we solve the problem of counting the number of all Schur rings over cyclic groups of prime power order and draw some parallels with Higman's PORC conjecture.

Keywords: Schur Ring, cyclic group, cyclotomic field, Catalan number, Schröder number, PORC conjecture

AMS Classification: 20C05, 11R18

1. Introduction

Let F be a field of characteristic zero, and let A denote an F-algebra. For any finite subset $C \subseteq A$, let $\overline{C} = \sum_{x \in C} x \in A$. Let G denote a finite group, and let $F[G]$ denote the group algebra of G with coefficients from F. We say that an element $\alpha \in F[G]$ is a *simple quantity* if there exists some subset $C \subseteq G$ such that $\alpha = \overline{C}$. Let $\{C_1, C_2, \ldots, C_r\}$ be a partition of a finite group G, and let S be the subspace of $F[G]$ spanned by $\overline{C_1}, \overline{C_2}, \ldots \overline{C_r}$, that is, S is spanned by simple quantities and contains the element $\overline{G}$. We say that S is a *Schur ring* [22, Wielandt] over G if

(1) $C_1 = \{1\}$,
(2) For each i, there is a j such that $(C_i)^{-1} = C_j$,
(3) For each i and j, $\overline{C_i} \cdot \overline{C_j} = \sum_{k=1}^{r} \lambda_{ijk} \overline{C_k}$, for $\lambda_{ijk} \in F$.

Schur rings were originally developed by Schur and Wielandt in the first half of the 20th century. Schur rings were first used to study permutation groups, but in later decades applications of Schur rings have emerged in combinatorics, graph theory, and design theory [8, 14].

As mentioned above, any Schur ring is uniquely determined by a partition of the elements of the group, although not every partition determines a Schur ring. An open question in the study of Schur rings is determining which partitions of the group induce a Schur ring and which ones do not. Much

work has be done to answer this question. In the case that our group G is cyclic, a complete classification has been found [11, 12]; see Theorem 3.3. In particular, the study of Schur rings over cyclic groups is a very active field with several recent papers being published on this topic: [9], [10], [11], [12], [16], [17], and [18].

In this paper we consider the problem of counting the number of Schur rings over Z_n, the cyclic group of order n. Although a structure theorem is available for Schur rings over cyclic groups, this still proves to be a difficult problem. Specializations of this problem have been considered before. For example, in [9] Kovács determines a formula to count the number of Schur rings over Z_{2^n} which are *wreath-indecomposable*, that is, those Schur rings which cannot be properly factored as a wreath product of Schur rings (see page 10). Kovács' formula involves the Catalan and Schröder numbers. We will see these again when we consider Schur rings over cyclic 2-groups in Section 6. In [13], Liskovets and Pöschel determine a formula for wreath-indecomposable Schur rings over Z_{p^n}, where p is an odd prime. This formula depends on the Catalan numbers and the number of divisors of $p-1$. We will also see these quantities again when we consider Schur rings over cyclic p-groups in Section 5.

A function f on a subset of integers S is called *polynomial on residue classes* or *PORC* if there exists a positive integer m and rational polynomials $p_0,\ p_1, \ldots, p_{m-1}$ such that, for all $x \in S$, $f(x) = p_a(x)$ whenever $x \equiv a \pmod{m}$ and $0 \leq a < m$. In other words, f acts like a polynomial on the residue classes modulo m. For a natural number n and prime number p, let $G(p,n)$ denote the number of isomorphism classes of groups of order p^n. The Higman's PORC conjecture states that for a fixed n and S is the set of primes $G(p,n)$ is a PORC function. Because a function on primes is PORC if and only if it is PORC on all but finitely many primes, it suffices to show that a function is PORC for sufficiently large primes. The conjecture has been varied for $n \leq 7$ and we include in Table 1.1 these polynomials (see [19, 20] and their references for the details).

Although Higman's PORC conjecture is likely untrue for $n \geq 10$ [2], various PORC conjectures have been proven for specific families of p-groups, e.g. [5, 6, 3, 24]. In the language of the PORC conjecture, Theorem 5.11 shows that the number of Schur rings over a cyclic p-group is satisfies the PORC conjecture for all n. We mention that the polynomials in Table 1.1 depend on powers of p and $\gcd(p-1,k)$ for various integers k. On the other hand, the polynomials for the number of Schur rings depends entirely only $d(p-1)$, the number of divisors of $p-1$ which we will simply abbreviate as x.

TABLE 1.1. $G(p,n)$ for $n \leq 7$

n	$G(p,n)$
1	1
2	2
3	5
4	15 if $p \geq 3$
5	$2p + 61 + 2\gcd(p-1,3) + \gcd(p-1,4)$ if $p \geq 5$
6	$3p^2 + 39p + 344 + 24\gcd(p-1,3) + 11\gcd(p-1,4) + 2\gcd(p-1,5)$ if $p \geq 5$
7	$3p^5 + 12p^4 + 44p^3 + 170p^2 + 707p + 2455$ $+ (4p^2 + 44p + 291)\gcd(p-1,3) + (p^2 + 19p + 135)\gcd(p-1,4)$ $+ (3p + 31)\gcd(p-1,5) + 4\gcd(p-1,7) + 5\gcd(p-1,8) + \gcd(p-1,9)$ if $p \geq 7$

2. Orbit Algebras and Cyclotomic Fields

Let A be an algebra over a field F and let $\mathcal{H} \leq \mathrm{Aut}_F(A)$ be finite, where $\mathrm{Aut}_F(A)$ is the group of F-algebra automorphisms of A. Let

$$A^{\mathcal{H}} = \{\alpha \in A : \sigma(\alpha) = \alpha, \text{ for all } \sigma \in \mathcal{H}\}.$$

Then $A^{\mathcal{H}}$ is a subalgebra of A and is referred to as an *orbit algebra*. The orbit algebra $A^{\mathcal{H}}$ is, in fact, the largest subalgebra of A that is fixed by all elements of $\mathcal{H}$. Such subalgebras appear frequently in mathematics, especially in Galois theory.

Suppose $\mathcal{B} \subseteq A$ such that $A = \mathrm{Span}_F(\mathcal{B})$. For each $\alpha \in A$, let $\mathcal{O}_\alpha = \{\sigma(\alpha) : \sigma \in \mathcal{H}\}$ denote the orbit of α in A with respect to $\mathcal{H}$ and let

$$\overline{\mathcal{O}_\alpha} = \sum_{\beta \in \mathcal{O}_\alpha} \beta$$

denote the *period* of α with respect to $\mathcal{H}$. Then $A^{\mathcal{H}} = \text{Span}_F\{\overline{\mathcal{O}_\alpha} : \alpha \in \mathcal{B}\}$, that is, $A^{\mathcal{H}}$ is spanned by the periods of a spanning set of A. This fact is the reason orbit algebras have their name.

One example of orbit algebras that will be of use in this paper will be the subfields of a cyclotomic field. Let $\zeta_n = e^{2\pi i/n} \in \mathbb{C}$, a primitive nth root of unity, and let $\mathcal{K}_n = \mathbb{Q}(\zeta_n) \subseteq \mathbb{C}$, the corresponding cyclotomic field. Let $\mathcal{G}_n$ denote the Galois group of $\mathcal{K}_n$ over $\mathbb{Q}$. When the context is clear, the subscripts may be omitted. From Galois theory, we know there is a one-to-one correspondence between the subfields of $\mathcal{K}_n$ and the subgroups of $\mathcal{G}_n$. Since every subalgebra of a field is likewise a field, there is a natural correspondence between the $\mathbb{Q}$-subalgebras of $\mathcal{K}_n$ and the subgroups of $\mathcal{G}_n$. In particular, if $\mathcal{H} \leq \mathcal{G}_n$, then $\mathcal{K}_n^{\mathcal{H}} = \mathbb{Q}(\overline{\mathcal{O}_{\zeta_n^i}} : 0 \leq i < n)$. By Galois correspondence, every subfield of $\mathcal{K}_n$ is of this form.

Every automorphism on $\mathcal{K}_n$ is determined by the image of ζ_n, which must be a primitive nth root. Therefore, $\mathcal{G}_n \cong (\mathbb{Z}/n\mathbb{Z})^*$, where $(\mathbb{Z}/n\mathbb{Z})^*$ denotes the multiplicative subgroup of the ring $\mathbb{Z}/n\mathbb{Z}$ consisting of congruence classes relatively prime to n. For each integer m relatively prime to n, let σ_m denote the automorphism in $\mathcal{G}_n$ which is determined by m. The group $(\mathbb{Z}/n\mathbb{Z})^*$ is, of course, well-known.

Lemma 2.1.

(a) $(\mathbb{Z}/2^k\mathbb{Z})^* \cong Z_2 \times Z_{2^{k-2}}$, *for all* $k \geq 2$. *In the case that* $k = 1$, $(\mathbb{Z}/2\mathbb{Z})^* = 1$.

(b) $(\mathbb{Z}/p^k\mathbb{Z})^* \cong Z_{p^{k-1}(p-1)}$, *for* $k \geq 1$ *and* p *is an odd prime.*

(c) Let $n \geq 2$ *be an integer with prime factorization* $n = p_1^{k_1} \cdots p_r^{k_r}$ *and each* p_i *is a distinct prime. Then* $(\mathbb{Z}/n\mathbb{Z})^* \cong (\mathbb{Z}/p_1^{k_1}\mathbb{Z})^* \times \ldots \times (\mathbb{Z}/p_r^{k_r}\mathbb{Z})^*$.

For each divisor d of n, there is a natural quotient map $\mathcal{G}_n \to \mathcal{G}_d$ given by restriction, that is, each automorphism $\sigma : \mathcal{K}_n \to \mathcal{K}_n$ maps to its restriction $\sigma|_{\mathcal{K}_d} : \mathcal{K}_d \to \mathcal{K}_d$. Thus, each subgroup $\mathcal{H} \leq \mathcal{G}_n$ induces a unique subgroup of $\mathcal{G}_d$. By abuse of notation, we will denote this quotient group also as $\mathcal{H}$. Since $\mathcal{H}$ can be identified as a set of integers modulo n, we may also identify $\mathcal{H}$ with this same set of integers but instead modulo d. Then it follows from above that

$$\mathcal{K}_n^{\mathcal{H}} \cap \mathcal{K}_d = \mathcal{K}_d^{\mathcal{H}}. \tag{2.1}$$

Furthermore, $\mathcal{K}_d^{\mathcal{H}}$ is the maximal subfield of $\mathcal{K}_d$ contained in $\mathcal{K}_n^{\mathcal{H}}$.

Let $\mathcal{L}_n$ be the lattice of subfields of $\mathcal{K}_n$. In the case that n is a power of a prime, the lattice of subfields of $\mathcal{K}_n$ is naturally *layered* by the powers of the prime. Let the *0th layer* of $\mathcal{L}_{p^n}$ be $\mathcal{L}_0 = \{\mathbb{Q}\}$. For $k \geq 1$, the *kth layer* of $\mathcal{L}_{p^n}$ is $\mathcal{L}_{p^k} \setminus \mathcal{L}_{p^{k-1}}$. In particular, the layers form a partition of $\mathcal{L}_{p^n}$. The *top layer* of $\mathcal{L}_{p^n}$ is the nth layer. We define the *bottom layer* of $\mathcal{L}_{p^n}$ to be $\mathcal{L}_p$, which is the union of the 1st and 0th layers.

By Lemma 2.1, the Galois groups of powers of 2 behave differently from the Galois groups of powers of an odd prime. Thus, we must consider the two cases separately. We will address the odd prime case first, followed by the even case.

FIGURE 1. The Lattice of Subfields of $\mathbb{Q}(\zeta_{3^4})$.

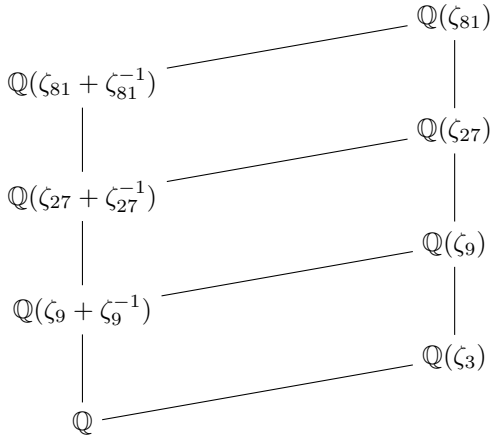
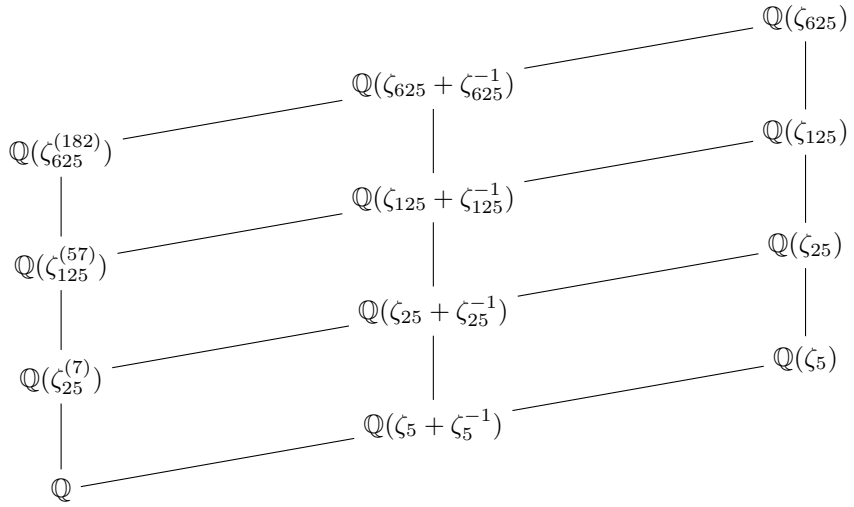
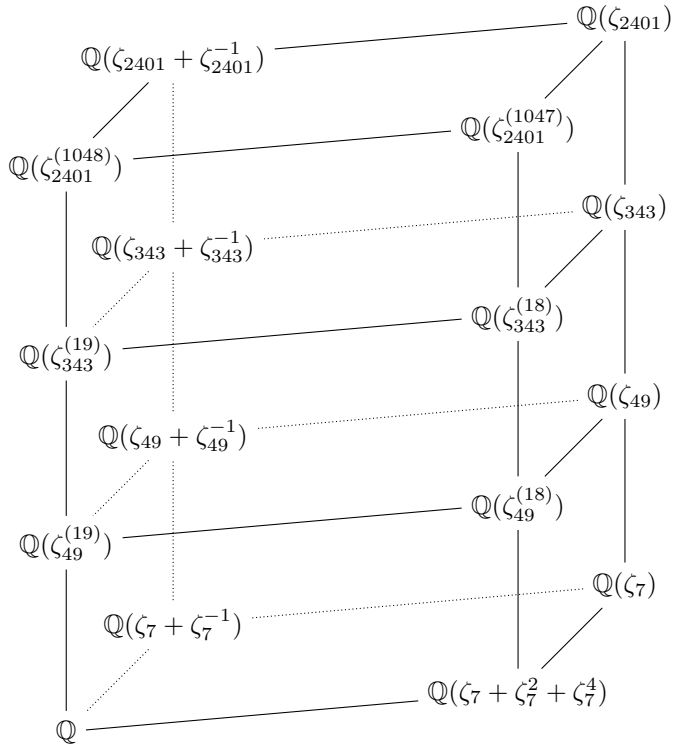


FIGURE 2. The Lattice of Subfields of $\mathbb{Q}(\zeta_{5^4})$.



Let us assume that p is an odd prime and let $\mathcal{G} = \mathcal{G}_{p^n}$. Then, by Lemma 2.1, $\mathcal{G}$ is a cyclic group. Thus, the subfields of $\mathcal{K}_{p^n}$ correspond to the divisors of $|\mathcal{G}|$. Now, $|\mathcal{G}| = p^n - p^{n-1} = p^{n-1}(p-1)$. Let x denote the number of divisors of $p-1$. Then $\mathcal{G}$ has nx subgroups. In particular, when $n = 1$, $\mathcal{K}_p$ has x subfields, or in other words, $|\mathcal{L}_p| = x$. By induction, the kth layer of $\mathcal{L}_{p^n}$ also contains exactly

FIGURE 3. The Lattice of Subfields of $\mathbb{Q}(\zeta_{7^4})$.



x subfields, for all $1 < k \leq n$. Furthermore, it follows by induction, elementary properties of cyclic groups, and basic Galois theory that each layer of $\mathcal{L}_{p^n}$ is lattice-isomorphic to the bottom layer, $\mathcal{L}_p$, and each successive layer sits atop its predecessor by a degree p extension, that is, if $\mathcal{H} \leq \mathcal{G}_{p^n}$ such that $\mathcal{K}_{p^n}^{\mathcal{H}}$ is in the top layer, then

$$[\mathcal{K}_{p^k}^{\mathcal{H}} : \mathcal{K}_{p^{k-1}}^{\mathcal{H}}] = p, \tag{2.2}$$

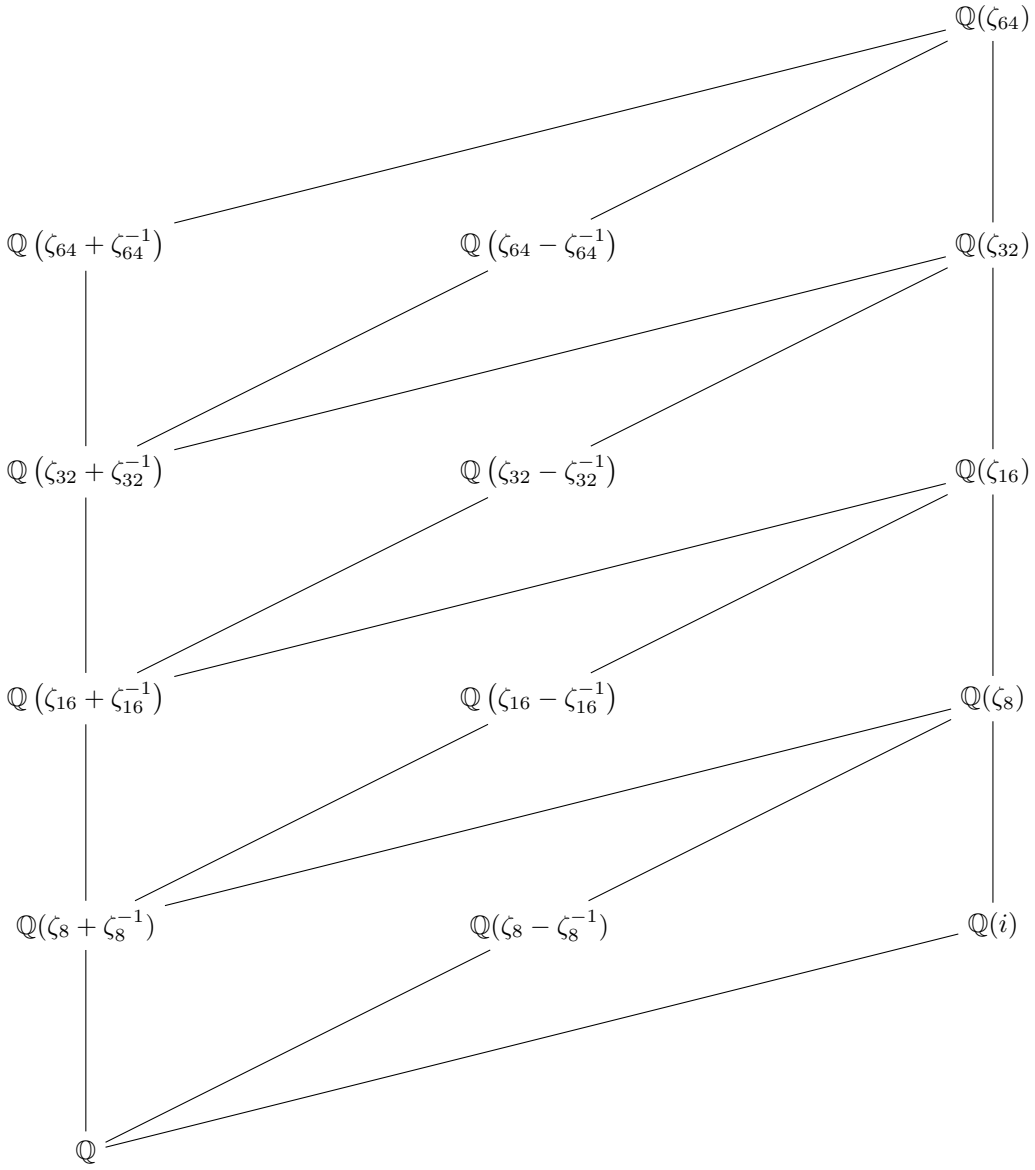
for all $1 < k \leq n$. Furthermore,

$$\left[\mathcal{K}_{p^n} : \mathcal{K}_{p^n}^{\mathcal{H}}\right] = \left[\mathcal{K}_{p^k} : \mathcal{K}_{p^k}^{\mathcal{H}}\right] \tag{2.3}$$

for all $1 \leq k \leq n$. These observations give a method to build the lattice of subfields for $\mathcal{K}_{p^n}$. Figures 1, 2, and 3 offer examples of the lattice $\mathcal{L}_{p^n}$ for primes $p = 3$, 5, and 7, respectively. In Figures 2 and 3, the element $\zeta_n^{(m)}$ denotes the period of ζ_n corresponding to the automorphism group generated by σ_m.

Next, we will switch our attention to the case when $p = 2$. As seen in Lemma 2.1, $\mathcal{G}_{2^n} \cong Z_2 \times Z_{2^{n-2}}$ for $n \geq 2$ and $\mathcal{G}_2 = 1$. In particular, $\mathcal{G}_4 \cong Z_2$, and hence $\mathcal{K}_4 = \mathbb{Q}(i)$ contains two subfields: $\mathbb{Q}(i)$ and $\mathbb{Q}$. For $\mathcal{K}_8$, we have that $\mathcal{G}_8 \cong Z_2 \times Z_2$, the Klein 4-group. Thus, $\mathcal{K}_8$ has 5 subfields: $\mathbb{Q}$, $\mathbb{Q}(i)$, $\mathbb{Q}(\zeta_8)$, $\mathbb{Q}(\zeta_8 + \zeta_8^{-1})$, and $\mathbb{Q}(\zeta_8 + \zeta_8^3)$.

FIGURE 4. The Lattice of Subfields of $\mathbb{Q}(\zeta_{64})$.



For the fourth layer of the lattice, we notice that $\mathcal{G}_{16} \cong Z_2 \times Z_4$ contains a copy of $Z_2 \times Z_2$ and hence contains three additional subgroups: two subgroups of order 4 and a subgroup of order 8. Thus, $\mathcal{L}_{16}$ contains three additional fields outside of $\mathcal{L}_8$ by Galois correspondence. These fields are in fact $\mathbb{Q}(\zeta_{16})$, $\mathbb{Q}(\zeta_{16}+\zeta_{16}^{-1})$, and $\mathbb{Q}(\zeta_{16}+\zeta_{16}^{7})$.

In general, $Z_2 \times Z_{2^{n-2}}$ has three more subgroups than $Z_2 \times Z_{2^{n-3}}$, and hence $\mathcal{L}_{2^n}$ has three more fields than $\mathcal{L}_{2^{n-1}}$ for $n \geq 3$. One of the fields is certainly $\mathbb{Q}(\zeta_{2^n})$. Since $\mathcal{G}_{2^n}$ is a 2-group, the remaining two fields must correspond to subgroups of $\mathcal{G}_{2^n}$ of order 2. The group $Z_2 \times Z_{2^{n-2}}$ has three elements of order 2. In particular, $\sigma_{2^n-1}, \sigma_{2^{n-1}-1}$, and $\sigma_{2^{n-1}+1}$ have order 2 in $\mathcal{G}_{2^n}$. But $\zeta^{2^{n-1}} = -1$. So, for the subgroup $\mathcal{H} = \langle \sigma_{2^{n-1}+1} \rangle$, $\overline{\mathcal{O}_\zeta} = \zeta + \zeta^{2^{n-1}+1} = \zeta - \zeta = 0$. Also, $\overline{\mathcal{O}_{\zeta^2}} = \overline{\mathcal{O}_{\zeta_{2^{n-1}}}} = \zeta_{2^{n-1}}$. Hence, $\mathbb{Q}(\zeta_{2^{n-1}}) \subseteq \mathbb{Q}(\zeta_{2^n})^{\mathcal{H}}$, which implies that $\mathbb{Q}(\zeta_{2^n})^{\mathcal{H}} = \mathbb{Q}(\zeta_{2^{n-1}})$ by degree considerations. Therefore, the additional two fields are $\mathbb{Q}(\zeta + \zeta^{-1})$ and $\mathbb{Q}(\zeta - \zeta^{-1})$.

Next, we notice that $\mathbb{Q}(\zeta_{2^n})^{\langle \sigma_{2^n-1} \rangle} \cap \mathbb{Q}(\zeta_{2^{n-1}}) = \mathbb{Q}(\zeta_{2^n})^{\langle \sigma_{2^n-1-1} \rangle} \cap \mathbb{Q}(\zeta_{2^{n-1}}) = \mathbb{Q}(\zeta_{2^{n-1}})^{\langle \sigma_{2^{n-1}-1} \rangle}$ $= \mathbb{Q}(\zeta_{2^{n-1}} + \zeta_{2^{n-1}}^{-1})$, by induction. Also, the automorphisms σ_{2^n-1} and $\sigma_{2^{n-1}-1}$ are contained in exactly one subgroup of order 4 in $\mathcal{G}_{2^n}$, which corresponds to $\mathbb{Q}(\zeta_{2^{n-1}} + \zeta_{2^{n-1}}^{-1})$. These observations lead to a method to build $\mathcal{L}_{2^n}$ for any n. In particular, each new layer of $\mathcal{L}_{2^n}$ contains three new fields: $\mathbb{Q}(\zeta_{2^n})$, $\mathbb{Q}(\zeta_{2^n} + \zeta_{2^n}^{-1})$, and $\mathbb{Q}(\zeta_{2^n} - \zeta_{2^n}^{-1})$, where the cyclotomic field $\mathbb{Q}(\zeta_{2^n})$ sits directly above the other two fields and $\mathbb{Q}(\zeta_{2^{n-1}})$ and where the fields $\mathbb{Q}(\zeta_{2^n} + \zeta_{2^n}^{-1})$ and $\mathbb{Q}(\zeta_{2^n} - \zeta_{2^n}^{-1})$ sit directly above $\mathbb{Q}(\zeta_{2^{n-1}} + \zeta_{2^{n-1}}^{-1})$. To illustrate, we construct $\mathcal{L}_{64}$ in Figure 4.

3. Schur Rings

Let S be a Schur ring over the finite group G afforded by the partition $\{C_1, C_2, \ldots, C_r\}$. The subsets $C_1, \ldots, C_r$ are called the *primitive sets* of S or *S-classes*. Let $\mathcal{D}(S)$ denote the set of S-classes. If $C \subseteq G$ and $\overline{C} \in S$, then C is called an *S-set*. If C is also a subgroup of G, then we say that C is an *S-subgroup* of G. If H is an S-subgroup, then let

$$S_H = \text{Span}_F\{\overline{C_i} : C_i \subseteq H\}.$$

Then S_H is a Schur ring over H.

Define additional operations on $F[G]$ as follows:

$$* : F[G] \to F[G] : \quad \left(\sum_{g \in G} \alpha_g g \right)^* = \sum_{g \in G} \alpha_g g^{-1}$$

and the *Hadamard product*

$$\circ : F[G] \times F[G] \to F[G] : \quad \left(\sum_{g \in G} \alpha_g g \right) \circ \left(\sum_{g \in G} \beta_g g \right) = \sum_{g \in G} \alpha_g \beta_g g.$$

Schur rings can then be characterized by these operations. For examples, the subspaces of $F[G]$ which are closed under $\circ$ are exactly those spanned by simple quantities.

Proposition 3.1 ([18] Lemma 1.3)**.** *Suppose that S is a subalgebra of $F[G]$. Then S is a Schur ring if and only if S is closed under $*$ and $\circ$ and $1, \overline{G} \in S$.*

Corollary 3.2. *Let S and T be Schur rings over G. Then $S \cap T$ is a Schur ring over G.*

Every finite group algebra $F[G]$ is a Schur ring, resulting from the partition of singletons on G. The partition $\{\{1\}, G \setminus \{1\}\}$ affords a *trivial Schur ring* over G, denoted $F[G]^0$.

Let $\mathcal{H} \leq \mathrm{Aut}(G)$ and

$$F[G]^{\mathcal{H}} = \{\alpha \in F[G] : \sigma(\alpha) = \alpha, \text{ for all } \sigma \in \mathcal{H}\}.$$

Then $F[G]^{\mathcal{H}}$ is a Schur ring afforded by the partition of G corresponding to the orbits of the $\mathcal{H}$-action on G. These Schur rings are referred to as *orbit Schur rings*. The center of $F[G]$ is an orbit Schur ring with $\mathcal{H} = \mathrm{Inn}(G)$. Let $\mathcal{R}(F[G]) = F[G]^{\mathrm{Aut}(G)}$ denote the *rational Schur ring*, whose primitive sets are the automorphism classes of G. For an abelian group G, let $\mathcal{S}(F[G]) = F[G]^{\langle * \rangle}$ denote the *symmetric Schur ring*, whose primitive sets are the inverse classes of G.

Let S and T be Schur rings over $F[G]$ and $F[H]$, respectively. We naturally can view G and H as subgroups of $G \times H$. Let

$$S \cdot T = \mathrm{Span}_F\{\overline{C} \cdot \overline{D} : C \in \mathcal{D}(S), D \in \mathcal{D}(T)\},$$

called the *dot product* of S and T. This forms a Schur ring with partition $\mathcal{D}(S \cdot T) = \{CD \subseteq G \times H : C \in \mathcal{D}(S), D \in \mathcal{D}(T)\}$. Furthermore, $S \cdot T \cong S \otimes_F T$, as F-algebras. Because of this fact, the Schur ring $S \cdot T$ is often called the tensor product of Schur rings.

The notion of *wedge product* of Schur rings presented below is originally based upon the presentation of Leung and Man [12], although it has been adapted from the original for the purposes of this paper.

Let $H \trianglelefteq G$ and let S be a Schur ring over G/H. Let $\pi : G \to G/H$ be the natural quotient map. Consider the partition of G given by $\mathcal{D} = \{\pi^{-1}(C) : C \in \mathcal{D}(S)\}$, that is, if $C = \{g_1H, g_2H, \ldots, g_kH\} \in \mathcal{D}(S)$, then $\pi^{-1}(C) = \bigcup_{i=1}^{k} g_iH \in \mathcal{D}$. Let $\pi^{-1}(S) = \mathrm{Span}_F\{\overline{D} : D \in \mathcal{D}\}$. Then $\pi^{-1}(S)$ is a subalgebra over $F[G]$ closed under $*$ and $\circ$ and contains $\overline{H}$ and $\overline{G}$, referred to as the *inflated Schur ring* of S over G. Let $\mathcal{D}(\pi^{-1}(S)) = \{\pi^{-1}(C) : C \in \mathcal{D}(S)\}$, which is a partition of G.

Let $H \trianglelefteq G$, and let S and T be Schur rings over H and G/H, respectively. Then

$$S \wr T = S + \pi^{-1}(T),$$

called the *wreath product* of S and T. The wreath product is likewise a Schur ring with partition $\mathcal{D}(S \wr T) = \mathcal{D}(S) \cup (\mathcal{D}(\pi^{-1}(T)) \setminus \{H\})$. It follows that $(S \wr T)_H = S$ and $\pi(S \wr T) = T$.

Let $1 < K \leq H < G$ be a sequence of finite groups such that $K \trianglelefteq G$. Let S be a Schur ring over H and T a Schur ring over G/K. Let $\pi : G \to G/K$ be the quotient map. Let

$$S \wedge_K T = S + \pi^{-1}(T),$$

which denotes the *wedge product* of S and T. When the context is clear, the subscript may be omitted. If we assume that H/K is a T-subgroup, K is an S-subgroup, and $\pi(S) = T_{H/K}$, then $S \wedge T$ is a Schur ring over G with partition $D(S \wedge T) = D(S) \cup (\mathcal{D}(\pi^{-1}(T)) \setminus \mathcal{D}(\pi^{-1}(T_{H/K})))$. Like above, it follows that $(S \wedge T)_H = S$ and $\pi(S \wedge T) = T$. If $H = K$, then $S \wedge T = S \wr T$. Thus, the wedge product of Schur rings is a generalized wreath product of Schur rings.

Let S be a Schur ring over G. If there exists subgroups $1 < K \leq H < G$, with $K \trianglelefteq G$, and Schur rings R and T over H and G/K, respectively, such that $S = R \wedge_K T$, then we say that S is *wedge-decomposable*; otherwise, we say that S is *wedge-indecomposable*. If S is wedge-decomposable, we call $1 < K \leq H < G$ a *wedge-decomposition* of S. We define the terms *wreath-decomposable*, *wreath-indecomposable*, and *wreath-decomposition* analogously.

Every wreath-decomposable Schur ring is clearly wedge-decomposable and every wedge-indecomposable Schur ring is wreath-indecomposable. On the other hand, there do exist Schur rings which are wreath-indecomposable but wedge-decomposable.

Let $Z_n = \langle z : z^n \rangle$ denote the cyclic group of order n. For each $d \mid n$, let L_d denote all elements of Z_n of order d. We will call this the dth *layer* of Z_n. Each layer is just an automorphism class of Z_n.

Leung and Man used the constructions of Schur rings mentioned above to classify all Schur rings over Z_n.

Theorem 3.3 ([11, 12])**.** *Let $G = Z_n$ and let S be a Schur ring over G. Then S is trivial, an orbit ring, a dot product of Schur rings, or a wedge product of Schur rings.*

Corollary 3.4. *Let $G = Z_{p^n}$, for some prime p, and let S be a Schur ring over G. Then S is trivial, an orbit ring, or a wedge product of Schur rings.*

Proof. Since G is a cyclic p-group, it cannot be expressed as a nontrivial direct product of groups. As a consequence, S cannot be expressed as a nontrivial dot product of Schur rings. The result then follows from Theorem 3.3. □

Corollary 3.5. *Let $G = Z_p$, for some prime p, and let S be a Schur ring over G. Then S is an orbit Schur ring.*

Proof. Since G has no nontrivial subgroups, S is wedge-indecomposable. Also, $F[G]^0 = \mathcal{R}(F[G])$. Thus, the result then follows from Corollary 3.4. □

Corollary 3.6. *Let $G = Z_{p^n}$. Then for any wedge-decomposable Schur ring S over G, there exists a wedge-decomposition $1 < K \leq H < G$ such that S_H is a wedge-indecomposable orbit algebra or a trivial Schur ring over H.*

Proof. By assumption, S has a wedge-decomposition $1 < K \leq H < G$. If S_H is wedge-decomposable, then it also has a wedge decomposition $1 < K' \leq H' < H$. Since K and K' are nontrivial subgroups of Z_{p^n}, $K \cap K'$ is likewise nontrivial. Next, every S-class outside of H is a union of cosets of K. So, every such S-class is also a union of cosets of $K \cap K'$. Similarly, every S-class inside of H but outside of H' is a union of cosets of $K \cap K'$. Therefore, $1 < K \cap K' \leq H' < G$ is a wedge-decomposition of S. It follows that a wedge-decomposition $1 < K \leq H < G$ of S can be chosen such that H is minimal. Such a choice implies that S_H must be wedge-indecomposable. By Corollary 3.4, S_H is either a trivial or orbit Schur ring. □

4. A Correspondence Between Schur Rings and Cyclotomic Fields

Every automorphism of Z_n is determined by $z \mapsto z^m$, and every automorphism on $\mathcal{K}_n$ is similarly determined by $\zeta \mapsto \zeta^m$, where m is unique modulo n and $\gcd(n, m) = 1$. Identifying these congruence classes provides an isomorphism between $\mathrm{Aut}(Z_n)$ and the Galois group $\mathcal{G}_n$.

Let $\omega_n : \mathbb{Q}[Z_n] \to \mathbb{Q}(\zeta_n)$ be the $\mathbb{Q}$-algebra map uniquely defined by the relation $\omega_n(z) = \zeta_n$. Let S be a Schur ring over $\mathbb{Q}[Z_n]$. Then $\omega_n(S)$ is a subalgebra of $\mathcal{K}_n$ and necessarily must be a subfield. From Galois theory, each subfield of $\mathcal{K}_n$ corresponds to a subgroup of $\mathcal{G}_n$. Likewise, each orbit Schur ring corresponds to a subgroup of $\mathrm{Aut}(Z_n) = \mathcal{G}_n$. This defines a one-to-one correspondence between the subfields of $\mathcal{K}_n$ and the orbit Schur rings of $\mathbb{Q}[Z_n]$. In fact, ω_n determines this correspondence. Since $\mathrm{Aut}(Z_n) = \mathcal{G}_n$, it holds that $\sigma_m \circ \omega_n = \omega_n \circ \sigma_m$. Hence, if $\mathcal{H} \leq \mathcal{G}_n$, then ω_n preserves $\mathcal{H}$-orbits and $\mathcal{H}$-periods, that is, $\omega_n(\overline{\mathcal{O}_{z^k}}) = \overline{\mathcal{O}_{\zeta^k}}$ for every $k \in \mathbb{Z}$. Since both $\mathbb{Q}[Z_n]^{\mathcal{H}}$ and $\mathcal{K}_n^{\mathcal{H}}$ are spanned by their $\mathcal{H}$-periods, we have

$$\omega_n(\mathbb{Q}[Z_n]^{\mathcal{H}}) = \mathcal{K}_n^{\mathcal{H}}. \tag{4.1}$$

Proposition 4.1. *Let $G = Z_n = \langle z \rangle$ and let $\mathcal{K} = \mathbb{Q}(\zeta_n)$. Then the lattice of orbit Schur rings over G is lattice-isomorphic via ω_n to the lattice of subfields of $\mathcal{K}$.*

Proof. Equation (4.1) shows that ω is clearly surjective onto the lattice of subfields. If $\omega(\mathbb{Q}[G]^{\mathcal{H}_1}) = \omega(\mathbb{Q}[G]^{\mathcal{H}_2})$ for $\mathcal{H}_1, \mathcal{H}_2 \leq \mathcal{G}$, then $\mathcal{K}^{\mathcal{H}_1} = \mathcal{K}^{\mathcal{H}_2}$, but the Fundamental Theorem of Galois theory implies

that $\mathcal{H}_1 = \mathcal{H}_2$. Therefore, ω is injective, which proves that ω is an isomorphism between these two lattices. $\square$

Corollary 4.2. *Let $\mathcal{H}_1, \mathcal{H}_2 \leq \mathcal{G}_n$. Then $\mathbb{Q}[Z_n]^{\mathcal{H}_1} = \mathbb{Q}[Z_n]^{\mathcal{H}_2}$ if and only if $\mathcal{H}_1 = \mathcal{H}_2$.*

According to Corollary 4.2, distinct automorphism subgroups of $\mathcal{G}_n$ produce distinct orbit Schur rings over Z_n. Corollary 4.2 is not true for arbitrary groups. For example, let $G = Z_4 \times Z_2 = \langle a, b \rangle$ and let

$$S = \mathrm{Span}_{\mathbb{Q}}\{1,\ a^2,\ b + a^2 b,\ a + a^3 + ab + ab^3\} \cong \mathbb{Q}Z_2 \wr \mathbb{Q}Z_2 \wr \mathbb{Q}Z_2.$$

In fact, $S = \mathcal{R}(\mathbb{Q}[G])$. Furthermore, the automorphism group $\mathrm{Aut}(G)$ is given by

$$\mathrm{Aut}(G) = \left\langle \sigma : \begin{smallmatrix} a \mapsto a \\ b \mapsto a^2 b \end{smallmatrix},\ \tau : \begin{smallmatrix} a \mapsto a^3 b \\ b \mapsto a^2 b \end{smallmatrix} \right\rangle \cong D_4.$$

Let $\mathcal{H} = \langle \tau \rangle \lneq \mathrm{Aut}(G)$. It can be shown that $\mathbb{Q}[G]^{\mathcal{H}} = \mathcal{R}(\mathbb{Q}[G]) = \mathbb{Q}[G]^{\mathrm{Aut}(G)}$, although $\mathcal{H} \neq \mathrm{Aut}(G)$.

Since $\mathbb{Q} \subseteq \mathbb{Q}[Z_n]^0 \subseteq \mathcal{R}(\mathbb{Q}[Z_n])$, (4.1) implies that

$$\mathbb{Q} = \omega(\mathbb{Q}) \subseteq \omega(\mathbb{Q}[Z_n]^0) \subseteq \omega(\mathcal{R}(\mathbb{Q}[Z_n])) = \mathbb{Q}.$$

Therefore,

$$\omega_n(\mathbb{Q}[Z_n]^0) = \mathbb{Q}. \tag{4.2}$$

If $\Phi_n(x) \in \mathbb{Z}[x]$ denotes the nth cyclotomic polynomial, then $\mathbb{Q}(\zeta_n) \cong \mathbb{Q}[x]/(\Phi_n(x))$. Since $\Phi_n(x) \mid (x^n - 1)$ and $\mathbb{Q}[Z_n] \cong \mathbb{Q}[x]/(x^n - 1)$, the quotient map $\mathbb{Q}[x] \to \mathbb{Q}(\zeta_n)$ factors as the composition $\mathbb{Q}[x] \to \mathbb{Q}[Z_n] \xrightarrow{\omega_n} \mathbb{Q}(\zeta_n)$. In particular, $\ker \omega_n = (\Phi_n(z)) \subseteq \mathbb{Q}[Z_n]$.

Lemma 4.3. *For each prime p dividing n, let Z_p denote the subgroup of Z_n of order p. Then $\ker \omega_n = (\overline{Z_p} : p \mid n) = \mathrm{Span}\{\overline{gZ_p} : p \mid n, g \in Z_n\}$. In particular, a simple quantity of $\mathbb{Q}[Z_n]$ is a kernel element if and only if it is a sum of unions of cosets of some non-trivial subgroups of G.*

Proof. Let $d \mid n$, and let $f_d(x) = \sum_{k=1}^{d} x^{n-kn/d}$. Then $\Phi_n(x)$ is the greatest common divisor of $\{f_p(x) : p \mid n,\ p \text{ is prime}\}$. Therefore, the ideal generated by the $f_p(x)$ is the principal ideal generated by $\Phi_n(x)$. In particular,

$$\ker \omega_n = (\Phi_n(z)) = (f_p(z) : p \mid n) = (\overline{Z_p} : p \mid n). \qquad \square$$

Let $S = S_H \wedge S_{G/K}$ be a wedge-decomposable Schur ring of $\mathbb{Q}[Z_n]$ with wedge decomposition $1 < K \leq H < G$. If $|H| = m$, then $\omega_n|_{\mathbb{Q}[H]} = \omega_m$. It then follows that $\omega_m(S_H) = \omega_n(S_H) \subseteq \omega_n(S)$.

Conversely, for any $C \in \mathcal{D}(S) \setminus \mathcal{D}(S_H)$, we see that $\overline{C}$ is a union of cosets of K and so $\omega(\overline{C}) = 0$, by Lemma 4.3. Therefore, $\omega(S) \subseteq \omega(S_H)$, which proves that

$$\omega_n(S_H \wedge S_{G/K}) = \omega_m(S_H). \tag{4.3}$$

For the remainder of the paper, we will focus on the case when $G = Z_{p^n}$ for a prime p.

The kernel $\ker(\omega_{p^n})$ becomes $(\overline{Z_p})$, which is spanned by the cosets of Z_p. Since $\ker(\omega_{p^n})$ is spanned by simple quantities, it is closed under the Hadamard product.

Proposition 4.4. *Let $G = Z_{p^n}$ for some prime p and let $\mathcal{R}(\mathbb{Q}[G]) = \mathbb{Q}[G]^{\mathcal{G}}$. Then $\mathcal{R}(\mathbb{Q}[G]) = \wr_{k=1}^{n} \mathbb{Q}[Z_p]^0$.*

Proof. Recall that L_d denotes the dth layer of G, that is, the subset of all elements of order d. Then $\mathcal{R}(\mathbb{Q}[G]) = \mathrm{Span}_{\mathbb{Q}}\{\overline{L_d} : d \mid p^n\} = \mathrm{Span}_{\mathbb{Q}}\{\overline{L_{p^k}} : 1 \le k \le n\}$. For $n = 1$, then $\mathcal{R}(G) = \mathbb{Q}[G]^0$. Assume that the result holds for each $k < n$. For each layer,

$$L_{p^k} = \bigcup_{g \in L_{p^k}} g Z_{p^{k-1}},$$

that is, L_{p^k} is the union of all nontrivial cosets of $Z_{p^{k-1}}$ in Z_{p^k}. Let $\pi : Z_{p^k} \to Z_{p^k}/Z_{p^{k-1}}$ be the natural map. Thus, $\mathrm{Span}\{\overline{Z_{p^{n-1}}}, \overline{L_{p^n}}\} = \pi^{-1}(\mathbb{Q}[Z_p]^0)$. Therefore, $\mathcal{R}(\mathbb{Q}[G]) = \mathrm{Span}\{\overline{L_{p^k}} : 0 \le k \le n-1\} \wr \mathbb{Q}[Z_p]^0$. But $\mathrm{Span}\{\overline{L_{p^k}} : 0 \le k \le n-1\} = \mathcal{R}(\mathbb{Q}[Z_{p^{n-1}}])$. So by induction,

$$\mathcal{R}(G) = \left(\wr_{i=0}^{n-1} \mathbb{Q}[Z_p]^0 \right) \wr \mathbb{Q}[Z_p]^0 = \wr_{k=1}^{n} \mathbb{Q}[Z_p]^0. \qquad \square$$

Theorem 4.5. *Let S_1 and S_2 be Schur rings over $Z_{p^{n_1}}$ and $Z_{p_{n_2}}$, respectively. Let $n = \max\{n_1, n_2\}$. So, S_1 and S_2 are subalgebras of $\mathbb{Q}[Z_{p^n}]$. Then*

$$\omega_n(S_1) \cap \omega_n(S_2) = \omega_n(S_1 \cap S_2).$$

Proof. For functions, it is always true that

$$\omega_n(S_1 \cap S_2) \subseteq \omega_n(S_1) \cap \omega_n(S_2).$$

Suppose that $\omega_n(S_1) = \mathbb{Q}$. Then

$$\mathbb{Q} \subseteq \omega_n(S_1 \cap S_2) \subseteq \omega_n(S_1) \cap \omega_n(S_2) = \mathbb{Q} \cap \omega_n(S_2) = \mathbb{Q}.$$

Therefore, $\omega_n(S_1 \cap S_2) = \omega_n(S_1) \cap \omega_n(S_2)$.

Let $i = 1, 2$. Suppose next that $\omega_n(S_i) = \mathcal{K}_n^{\mathcal{H}_i}$ for $\mathcal{H}_i \leq \mathcal{G}_n$. Let $H_i \leq Z_{p^{n_i}}$ such that H_i is minimal with respect to the property $\omega_n(S_i) = \omega((S_i)_{H_i})$. By Corollary 3.6 and (4.3), $(S_i)_{H_i} = \mathbb{Q}[Z_{p^{n_i}}]^{\mathcal{H}_i}$. Let $H = H_1 \cap H_2$ and $\mathcal{H} = \mathcal{H}_1\mathcal{H}_2$. Let $m = |H|$. Then

$$\begin{aligned}
\omega_n(S_1 \cap S_2) &\supseteq \omega_n((S_1)_{H_1} \cap (S_2)_{H_2}) \\
&= \omega_n(\mathbb{Q}[Z_{p^{n_1}}]^{\mathcal{H}_1} \cap \mathbb{Q}[Z_{p^{n_2}}]^{\mathcal{H}_2}) = \omega_n(\mathbb{Q}[H]^{\mathcal{H}}) \\
&= \mathcal{K}_m^{\mathcal{H}} = \mathcal{K}_{m_1}^{\mathcal{H}_1} \cap \mathcal{K}_{m_2}^{\mathcal{H}_2} = \omega_n(\mathbb{Q}[H_1]^{\mathcal{H}_1}) \cap \omega_n(\mathbb{Q}[H_2]^{\mathcal{H}_2}) \\
&= \omega_n((S_1)_{H_1}) \cap \omega_n((S_2)_{H_2}) = \omega_n(S_1) \cap \omega_n(S_2),
\end{aligned}$$

which finishes the proof. □

Corollary 4.6. *Let S be a Schur ring over Z_{p^n}. If $H = Z_d$ is an S-subgroup, then*

$$\omega(S) \cap \mathbb{Q}(\zeta_d) = \omega(S_H).$$

Proof. By Theorem 4.5, $\omega(S) \cap \mathbb{Q}(\zeta_d) = \omega(S) \cap \omega(\mathbb{Q}[H]) = \omega(S \cap \mathbb{Q}[H]) = \omega(S_H)$. □

Theorem 4.7. *Let $G = Z_{p^n}$ and let S be a Schur ring over G such that $\omega(S) = \mathbb{Q}$. Then there exists a subgroup $H \leq G$ and a Schur ring T over G/H such that $S = \mathbb{Q}[H]^0 \wr T$.*

Proof. By Corollary 3.4, S is trivial, an orbit ring, or wedge-decomposable. If S is trivial, then we are done. In the second case, by Proposition 4.1, $\mathcal{R}(\mathbb{Q}[G])$ is the unique Schur ring which maps onto $\mathbb{Q}$, which has the desired form by Proposition 4.4. Finally, suppose there exists S-subgroups $1 < K \leq H < G$ such that $S = S_H \wedge S_{G/K}$ and S_H is trivial or a wedge-indecomposable orbit Schur ring. But $\omega(S_H) = \omega(S) = \mathbb{Q}$. Since the only indecomposable orbit ring which maps onto $\mathbb{Q}$ is $S_H = \mathbb{Q}[Z_p]^0$, again by Proposition 4.4, in either case $S_H = \mathbb{Q}[H]^0$. Since K is a non-trivial S_H-subgroup, it must be that $K = H$. Therefore, $S = S_H \wr S_{G/H} = \mathbb{Q}[H]^0 \wr S_{G/H}$. □

Theorem 4.8. *Let S be a Schur ring over Z_{p^n} and $\omega(S) \in \mathcal{L}_{p^{n-1}} \setminus \{\mathbb{Q}\}$. Then S is wedge-decomposable.*

Proof. Let $G = Z_{p^n}$. Since $\omega(S)$ is not in the top layer of $\mathcal{L}_{p^n}$, there exists some subgroup $H \lneq G$ such that $\omega(S) \subseteq \omega(\mathbb{Q}[H])$ and H is chosen minimally. Then

$$\omega(S) = \omega(S) \cap \omega(\mathbb{Q}[H]) = \omega(S \cap \mathbb{Q}[H]) = \omega(S_H).$$

By the minimality of H, H must be an S-subgroup. Since $\omega(S_H) \neq \mathbb{Q}$, H must be a nontrivial subgroup of G. In particular, $\overline{G} - \overline{H} \in \ker(\omega|_S)$.

Since $\ker(\omega)$ and S are closed under the Hadamard product, $\ker(\omega|_S) = \ker(\omega) \cap S$ is likewise closed under $\circ$. Let $C \in \mathcal{D}(S) \setminus \mathcal{D}(S_H)$. Since $\omega(S) = \omega(S_H)$, there exists some $\alpha \in S_H$ such that $\omega(\overline{C}) = \omega(\alpha)$. Thus, $\overline{C} - \alpha \in \ker(\omega|_S)$. Therefore, $\overline{C} = (\overline{C} - \alpha) \circ (\overline{G} - \overline{H}) \in \ker(\omega|_S)$. Since $\overline{C}$ is a simple quantity, Lemma 4.3 implies that C is a union of cosets of some subgroup. This subgroup is exactly the maximal subset of G which stabilizes C. A result due to Wielandt [23] states that these stabilizers are S-subgroups. Taking intersections if necessary, every class $C \in \mathcal{D}(S) \setminus \mathcal{D}(S_H)$ is a union of cosets of some nontrivial S-subgroup K. Therefore, S is wedge-decomposable. □

Theorem 4.9. *Let S be a Schur ring over Z_{p^n} such that $\omega(S)$ is in the top layer of $\mathcal{L}_{p^n}$. Then S is an orbit Schur ring, and hence S is the unique Schur ring over Z_{p^n} which maps to $\omega(S)$.*

Proof. By (4.2) and (4.3) if S is trivial or wedge-decomposable then $\omega(S)$ is not in the top layer. Thus, S is an orbit Schur ring. By Proposition 4.1, S is the unique orbit Schur ring mapping onto $\omega(S)$. □

5. Counting Schur Rings over Cyclic p-Groups

Using the representation $\omega_n : \mathbb{Q}[Z_n] \to \mathbb{Q}(\zeta_n)$ which was considered in the previous chapter, we will construct a recursive formula and generating function for the integer sequence counting the number of Schur rings over Z_{p^n}, for p a odd prime.

Definition 5.1. Let $\Omega(n)$ denote the number of Schur rings over Z_{p^n} and let $\Omega(n,k)$ denote the number of Schur rings S over Z_{p^n} such that $\omega(S) = \mathcal{K}_{p^k}$.

We have that $\Omega(0) = 1$ since there is exactly one Schur ring over $Z_{p^0} = 1$, the group ring itself. Also, if x denotes the number of divisors of $p-1$, then $\Omega(1) = x$ by Corollary 3.5.

Proposition 5.2. *The number of Schur rings over Z_{p^n}, for $n \geq 1$, mapping onto $\mathbb{Q}$ with respect to ω is equal to the sum of the number of Schur rings over Z_{p^k} for $0 \leq k \leq n-1$, that is,*

$$\Omega(n,0) = \sum_{k=0}^{n-1} \Omega(k). \tag{5.1}$$

Proof. Let $G = Z_{p^n}$. By Theorem 4.7, if $\omega(S) = \mathbb{Q}$ then $S = \mathbb{Q}[Z_{p^k}]^0 \wr T$ for some Schur ring T over G/Z_{p^k}. If we consider the trivial Schur ring on G as a trivial wreath product, that is, $\mathbb{Q}[G]^0 = \mathbb{Q}[G]^0 \wr \mathbb{Q}[1]$, then every Schur ring descending to $\mathbb{Q}$ has the form

$$S = \mathbb{Q}[Z_{p^k}]^0 \wr T,$$

where $1 \leq k \leq n$ and T ranges over all the Schur rings of $G/Z_{p^k} \cong Z_{p^{n-k}}$. Since every Schur ring over G of this form maps to $\mathbb{Q}$, the proof is finished. □

Proposition 5.3. *The number of Schur rings over Z_{p^n} mapping to $\mathcal{K}_p$ with respect to ω is equal to the number of Schur rings over $Z_{p^{n-1}}$, that is,*

$$\Omega(n,1) = \Omega(n-1). \tag{5.2}$$

Proof. Let $G = Z_{p^n}$. If $n = 1$, then $\Omega(n-1) = \Omega(0) = 1$. By Corollary 3.5, there is only one Schur ring which maps to $\mathcal{K}_p$. So the result follows.

Suppose that $n \geq 2$. Let S be the orbit Schur ring over $G = Z_{p^n}$ which maps onto $\mathcal{K}_p$. By Theorem 4.8, S is wedge-decomposable. By Corollary 3.6, there is a wedge decomposition of S, $1 < K \leq H < Z_{p^n}$, such that S_H is trivial or an indecomposable orbit Schur ring. By Proposition 4.3, $\omega(S) = \omega(S_H)$. If S_H is trivial, then $\omega(S_H) = \mathbb{Q}$, by Proposition 4.2. Thus, S_H is an indecomposable orbit Schur ring. Now, if $Z_p \neq H$, then S_H is wedge-decomposable by Theorem 4.8. Therefore, $H = Z_p$, which forces $K = H$. In fact, $S_H = \mathbb{Q}[Z_p]$. This shows that $S = \mathbb{Q}[Z_p] \wr T$, where T is some Schur ring over G/Z_p. Since every Schur ring over G of this form maps to $\mathcal{K}_p$, the proof is finished. □

Proposition 5.4. *The number of Schur rings over Z_{p^n} mapping to $\mathcal{K}_{p^n}$ with respect to ω is one, that is,*

$$\Omega(n,n) = 1. \tag{5.3}$$

Proof. Since $\mathcal{K}_{p^n}$ is a field in the top layer, this formula follows immediately from Theorem 4.9. □

Proposition 5.5. *For $n \geq 2$, the number of Schur rings over Z_{p^n} mapping to $\mathcal{K}_{p^k}$ for $1 < k \leq n$ with respect to ω is equal to the sum of the number of Schur rings over $Z_{p^{n-1}}$ mapping onto $\mathcal{K}_{p^j}$ where j ranges between $k-1$ and $n-1$, that is,*

$$\Omega(n,k) = \sum_{j=k-1}^{n-1} \Omega(n-1,j). \tag{5.4}$$

Proof. Let $G = Z_{p^n}$. If $k = n$, then $\Omega(n,n) = 1 = \Omega(n-1,n-1)$, by (5.3). If $1 < k < n$, then each Schur ring mapping onto $\mathcal{K}_{p^n}$ is wedge-decomposable, by Theorem 4.8. In particular, if S is a Schur ring over Z_{p^n} such that $\omega(S) = \mathcal{K}_{p^k}$, then there exists a wedge-decomposition such that $1 < K \leq H = Z_{p^k} < G$ and $S_H = \mathbb{Q}[H]$. Put another way, $S = \mathbb{Q}[H] \wedge T$, where T is a Schur ring over G/K. Clearly, $\overline{K} \in \mathbb{Q}[H]$ for any choice of K. If $\pi : G \to G/K$ is the quotient map, then $\pi(\mathbb{Q}[H]) = \mathbb{Q}[H/K]$. Therefore, the wedge product $\mathbb{Q}[H] \wedge T$ is possible if and only if H/K is a T-subgroup and $T_{H/K} = \mathbb{Q}[H/K]$. Without the loss of generality, we may assume that $K = Z_p$, since any coset of K is necessarily a coset of Z_p. If we identify π with the map $\pi : Z_{p^n} \to Z_{p^{n-1}}$, then $\pi(H) = Z_{p^{k-1}}$ and we must determine which Schur rings T have the property that $T_{H/K} = \mathbb{Q}[Z_{p^{k-1}}]$. Now, $\omega(T_{H/K}) = \mathcal{K}_{p^{k-1}}$, but by Corollary 4.6 we

have $\omega(T_{H/K}) = \omega(T) \cap \mathcal{K}_{p^{k-1}}$. Equation (2.1) then gives that $\omega(T) = \mathcal{K}_{p^j}$ for some $k-1 \leq j \leq n-1$. Since every Schur ring of this type can be wedged to $\mathbb{Q}[H]$, the equality is proven. □

Proposition 5.6. *Let $E, F \in \mathcal{L}_{p^k} \setminus \mathcal{L}_{p^{k-1}}$. Then the number of Schur rings over Z_{p^n} which map onto E with respect to ω is equal to the number of Schur rings over Z_{p^n} which map onto F with respect to ω. In particular, the number of Schur rings mapping onto E is equal to $\Omega(n,k)$.*

Remember that $\mathbb{Q} \in \mathcal{L}_{p^0}$ and is contained in the 0th layer of $\mathcal{L}_{p^n}$, not the first layer $\mathcal{L}_p \setminus \mathcal{L}_1$.

Proof. Let $\Omega(n,E)$ be the number of Schur rings over Z_{p^n} which map onto E. If $k = 0$, then the only field in this layer is $\mathbb{Q}$. So, $E = \mathbb{Q}$. If $k = 1$, we can mimic the proof of Proposition 5.3 to get $\Omega(n,E) = \Omega(n-1) = \Omega(n,1)$. So, we may suppose that $k \geq 2$.

We will now induct on n. Let $n = 2$. Then the only k to consider is $k = 2$, which represents the top layer. Mimicking the proof of Proposition 5.4, we get $\Omega(n,E) = 1 = \Omega(n,k)$. Suppose now that the result holds for all integers less than n. Mimicking the the proof of Proposition 5.5 (using here also (2.3)), we have

$$\Omega(n,E) = \sum_{j=k-1}^{n-1} \Omega(n-1, E \cap \mathcal{K}_{p^j}).$$

By induction, $\Omega(n-1, E \cap \mathcal{K}_{p^j}) = \Omega(n-1,j)$ for each j, which proves $\Omega(n,E) = \Omega(n,k)$. □

Theorem 5.7. *The number of Schur rings over Z_{p^n}, where p is an odd prime and $n \geq 2$, is given by the following equation:*

$$\Omega(n) = \Omega(n,0) + (x-1)\Omega(n,1) + x\sum_{k=2}^{n} \Omega(n,k), \tag{5.5}$$

where x denotes the number of divisors of $p-1$.

Proof. There is exactly one field in the 0th layer, $(x-1)$ fields in the first layer, and x fields in all remaining layers of $\mathcal{L}_{p^n}$. The equation then follows from Proposition 5.6. □

Equation (5.5) provides for us a formula which can calculate the number of Schur rings over Z_{p^n} using $\Omega(n,k)$ for $k \leq n$. This then begs the question, "How does one compute $\Omega(n,k)$?" Equations (5.1), (5.2), and (5.3) provides answers to this question when $k = 0$, 1, and n. For example, we can use (5.5) to compute $\Omega(2)$:

$$\begin{aligned} \Omega(2) &= \Omega(2,0) + (x-1)\Omega(2,1) + x\Omega(2,2) \\ &= (\Omega(0) + \Omega(1)) + (x-1)\Omega(1) + x \\ &= (1+x) + (x-1)x + x \end{aligned}$$

$$= \quad x^2 + x + 1.$$

Using (5.4), we can compute all remaining values of $\Omega(n,k)$ recursively. We provide a few examples below.

Corollary 5.8. *For $n \geq 2$,*

$$\Omega(n, n-1) = x + (n-2). \tag{5.6}$$

Proof. We proceed by induction on n. For $n = 2$, we have $\Omega(2,1) = \Omega(1) = x = x + (2-2)$. For $n > 2$, we have

$$\begin{aligned}
\Omega(n, n-1) &= \Omega(n-1, n-2) + \Omega(n-1, n-1) \quad \text{by (5.4)}, \\
&= \Omega(n-1, (n-1)-1) + 1 \quad \text{by (5.3)}, \\
&= x + (n-3) + 1 \quad \text{by induction}, \\
&= x + (n-2). \qquad \square
\end{aligned}$$

Corollary 5.9. *For $n \geq 3$,*

$$\Omega(n, n-2) = x^2 + (n-2)x + \binom{n-1}{2}. \tag{5.7}$$

Proof. We proceed by induction on n. For $n = 3$, we have $\Omega(3,1) = \Omega(2) = x^2 + x + 1 = x^2 + (3-2)x + \binom{3-1}{2}$. For $n > 3$, we have

$$\begin{aligned}
\Omega(n, n-2) &= \Omega(n-1, n-3) + \Omega(n-1, n-2) + \Omega(n-1, n-1) \\
&= \Omega(n-1, (n-1)-2) + \Omega(n-1, (n-1)-1) + 1 \\
&= \left(x^2 + (n-3)x + \frac{(n-3)(n-2)}{2} \right) + (x + (n-3)) + 1 \\
&= x^2 + (n-2)x + \binom{n-1}{2}. \qquad \square
\end{aligned}$$

By a similar induction argument, we can also prove the identity

$$\Omega(n, n-3) = x^3 + (n-2)x^2 + \left(\binom{n-1}{2} + 1 \right) x + \left(\binom{n}{3} - 3 \right) \tag{5.8}$$

for $n \geq 4$. As in the previous proofs, the base case of the induction argument uses the calculation of $\Omega(3)$, which can be computed using $\Omega(3,3)$, $\Omega(3,2)$, $\Omega(3,1)$ and $\Omega(3,0)$. Thus, $\Omega(n)$ can be computed using $\Omega(n,k)$, which can be computed using $\Omega(j)$ for $j < n$. Therefore, there is a recursive procedure to compute $\Omega(n)$ from $\Omega(j)$ for $j < n$. We now will work to unearth this recursive formula.

FIGURE 5. The first several values of $\Omega(n,k)$

$$\begin{aligned}
\Omega(1,\cdot) &= 1\\
\Omega(2,\cdot) &= x,\ 1\\
\Omega(3,\cdot) &= x^2+x+1,\ x+1,\ 1\\
\Omega(4,\cdot) &= x^3+2x^2+4x+1,\ x^2+2x+3,\ x+2,\ 1\\
\Omega(5,\cdot) &= x^4+3x^3+8x^2+9x+2,\ x^3+3x^2+7x+7,\ x^2+3x+6,\ x+3,\ 1\\
\Omega(6,\cdot) &= x^5+4x^4+13x^3+23x^2+25x+3,\ x^4+4x^3+12x^2+20x+9,\ x^3+4x^2+11x+17,\ x^2+4x+10,\\
&\quad x+4,\ 1\\
\Omega(7,\cdot) &= x^6+5x^5+19x^4+44x^3+72x^2+69x+5,\ x^5+5x^4+18x^3+40x^2+61x+54,\ x^4+5x^3+17x^2+36x+51,\\
&\quad x^3+5x^2+16x+32,\ x^2+5x+15,\ x+5,\ 1\\
\Omega(8,\cdot) &= x^7+6x^6+26x^5+73x^4+152x^3+222x^2+203x+8,\ x^6+6x^5+25x^4+68x^3+135x^2+188x+163,\\
&\quad x^5+6x^4+24x^3+63x^2+119x+158,\ x^4+6x^3+23x^2+58x+109,\ x^3+6x^2+22x+53,\\
&\quad x^2+6x+21,\ x+6,\ 1
\end{aligned}$$

Using (5.1) and (5.2), we can rewrite (5.5) as

$$\Omega(n) = x\Omega(n-1) + \sum_{k=0}^{n-2}\Omega(k) + x\sum_{k=2}^{n}\Omega(n,k). \tag{5.9}$$

Thus, we need to expand $\sum_{k=2}^{n}\Omega(n,k)$ using (5.4). This will produce an equation of the following form:

$$\sum_{i=2}^{n}\Omega(n,i) = \sum_{i=1}^{n-1}c_i\Omega(n-i,1) = \sum_{i=2}^{n}c_{i-1}\Omega(n-i) \tag{5.10}$$

for some positive integers c_i. In particular, the jth iteration of (5.4) will produce an equation of the form

$$\sum_{k=2}^{n}\Omega(n,k) = \sum_{i=1}^{j-1}c_i\Omega(n-i,1) + \sum_{k=j+1}^{n}c_{jk}\Omega(n-j,k-j) \tag{5.11}$$

for some positive integers c_{jk}. We note that $c_{i(i+1)} = c_i$ and $c_{0k} = 1$ for all k. Furthermore,

$$c_{jk} = \sum_{\ell=j}^{k}c_{(j-1)\ell} \tag{5.12}$$

by Proposition 5.5. When $0 < j < k-1$, (5.12) can be rewritten recursively to give

$$c_{jk} = c_{(j-1)k} + \sum_{\ell=j}^{k-1}c_{(j-1)\ell} = c_{(j-1)k} + c_{j(k-1)}. \tag{5.13}$$

From (5.13), we can create a triangular array of integers, depicted in Figure 6, where k indexes the rows ($k \geq 1$) and j indexes the columns ($0 \leq j < k$). The diagonal entries of the triangle give the values of c_i.

FIGURE 6. The Triangular Array of c_{jk} Coefficients

1							
1	2						
1	3	5					
1	4	9	14				
1	5	14	28	42			
1	6	20	48	90	132		
1	7	27	75	165	297	429	
1	8	35	110	275	572	1001	1430

Lemma 5.10. *Let c_i be the coefficients given in Equation* (5.10)*. Then $c_i = \frac{1}{i+1}\binom{2i}{i}$, that is, c_i is the ith Catalan number.*

Proof. For convenience, we define $c_{00} = 1$ and $c_{jj} = c_{(j-1)j}$ for $j > 0$. This extended triangular array is known as Catalan's Triangle. One property of Catalan's Triangle is that the sequence of diagonal entries is the sequence of Catalan numbers [21]. □

Theorem 5.11. *The number of Schur rings over Z_{p^n}, where p is an odd prime and $n \geq 1$, is given by the following recursive equation:*

$$\Omega(n) = x\Omega(n-1) + \sum_{k=2}^{n}(c_{k-1}x + 1)\Omega(n-k), \tag{5.14}$$

where $\Omega(0) = 1$, $\Omega(1) = x$ denotes the number of divisors of $p-1$, and $c_k = \frac{1}{k+1}\binom{2k}{k}$ is the kth Catalan number.

For $n = 1$, we are considering the sum in (5.14) to be empty.

Proof. The statements $\Omega(0) = 1$ and $\Omega(1) = x$ have already been proven. For $n \geq 2$,

$$\begin{aligned}
\Omega(n) &= x\Omega(n-1) + \sum_{k=0}^{n-2} \Omega(k) + x \sum_{k=2}^{n} \Omega(n,k), \quad \text{by (5.9)}, \\
&= x\Omega(n-1) + \sum_{k=0}^{n-2} \Omega(k) + x \sum_{k=2}^{n} c_{k-1}\Omega(n-k), \quad \text{by (5.10)}, \\
&= x\Omega(n-1) + \sum_{k=2}^{n} (c_{k-1}x + 1)\Omega(n-k).
\end{aligned}$$

Finally, the formula follows from Lemma 5.10. □

By (5.14), $\Omega(n)$ can be computed recursively without reference to $\Omega(n,k)$ and makes for a much more efficient recurrence. The first several values of $\Omega(n)$ are listed in Figure 7. Now, $\Omega(n)$ is a polynomial of x. Thus, the number of Schur rings over $\mathbb{Z}_{p^n}$ is computed by evaluating this polynomial for a specific value of x which depends on the prime p. Table 5.1 lists the number of Schur rings over Z_{p^n} up to the tenth power for the first seven odd primes.

FIGURE 7. The first several Ω-polynomials

$$\begin{aligned}
\Omega(1) &= x \\
\Omega(2) &= x^2 + x + 1 \\
\Omega(3) &= x^3 + 2x^2 + 4x + 1 \\
\Omega(4) &= x^4 + 3x^3 + 8x^2 + 9x + 2 \\
\Omega(5) &= x^5 + 4x^4 + 13x^3 + 23x^2 + 25x + 3 \\
\Omega(6) &= x^6 + 5x^5 + 19x^4 + 44x^3 + 72x^2 + 69x + 5 \\
\Omega(7) &= x^7 + 6x^6 + 26x^5 + 73x^4 + 152x^3 + 222x^2 + 203x + 8 \\
\Omega(8) &= x^8 + 7x^7 + 34x^6 + 111x^5 + 275x^4 + 511x^3 + 703x^2 + 623x + 13 \\
\Omega(9) &= x^9 + 8x^8 + 43x^7 + 159x^6 + 452x^5 + 997x^4 + 1725x^3 + 2272x^2 + 1990x + 21 \\
\Omega(10) &= x^{10} + 9x^9 + 53x^8 + 218x^7 + 695x^6 + 1754x^5 + 3572x^4 + 5854x^3 + 7510x^2 + 6559x + 34
\end{aligned}$$

Examining Figure 7, one can recognize a few patterns with these polynomials. First, $\Omega(n)$ is always a monic degree n polynomial. Next, the coefficient of x^{n-1} is always $n - 1$. Both of these statements can be easily proven by induction. Other statements about the coefficients of $\Omega(n)$ can also be stated and proven. Perhaps the most surprising sequence of coefficients is the sequence of constant terms.

TABLE 5.1. Number of Schur Rings over Z_{p^k}

$k\backslash p$	**3**	**5**	**7**	**11**	**13**	**17**	**19**
1	2	3	4	4	6	5	6
2	7	13	21	21	43	31	43
3	25	58	113	113	313	196	313
4	92	263	614	614	2,288	1,247	2,288
5	345	1,203	3,351	3,351	16,749	7,953	16,749
6	1,311	5,531	18,329	18,329	122,675	50,775	122,675
7	5,030	25,511	100,372	100,372	898,706	324,323	898,706
8	19,439	117,910	550,009	550,009	6,584,443	2,072,078	6,584,443
9	75,545	545,730	3,015,021	3,015,021	48,243,393	13,239,896	48,243,393
10	294,888	2,528,263	16,531,326	16,531,326	353,479,684	84,603,579	353,479,684

Corollary 5.12. *Let p be an odd prime. Then let $f_n(x) = \Omega(n) \in \mathbb{Z}[x]$. Then $f_n(0) = F_{n-1}$, where F_n is the nth term of the Fibonacci sequence.*

Proof. First, we claim that $F_n = 1 + \sum_{k=0}^{n-2} F_k$ for $n \geq 2$. For $n = 2$, we get $F_2 = 1 + F_0 = 1 + 0 = 1$. For $n > 2$, we get $F_n = F_{n-1} + F_{n-2} = \left(1 + \sum_{k=0}^{n-3} F_k\right) + F_{n-2} = 1 + \sum_{k=0}^{n-2} F_k$, which proves the claim.

It is easy enough to see that $f_1(0) = 0 = F_0$ and $f_2(0) = 1 = F_1$. Suppose that $f_k(0) = F_{k-1}$ for all $k < n$. By (5.14),

$$f_n(0) = \sum_{k=2}^{n} f_{n-k}(0) = \sum_{k=0}^{n-2} f_k(0) = 1 + \sum_{k=1}^{n-2} f_k(0) = 1 + \sum_{k=1}^{n-2} F_{k-1} = 1 + \sum_{k=0}^{n-3} F_k = F_{n-1}. \qquad \square$$

Let $\mathcal{F}(z) = \sum_{n=0}^{\infty} \Omega(n) z^n$ be the generating function of Ω. Using

$$\mathcal{C}(z) = \sum_{n=0}^{\infty} c_n z^n = \frac{1 - \sqrt{1-4z}}{2z},$$

the generating function for the Catalan numbers, and the usual generating function calculations, one computes that

$$\mathcal{F}(z) = \frac{2(1-z)}{-2z^2 + (x-2)z - (x-2) + x(1-z)\sqrt{1-4z}} \tag{5.15}$$

Now, one can continue working with the generating function of $\Omega(n)$ using the typical combinatorial methods to produce a non-recursive formula for $\Omega(n)$. Unfortunately, this formula is highly complicated, so we will be content with (5.14).

6. Counting Schur Rings Over Cyclic 2-groups

As is common practice, the case $p = 2$ must be treated separately from all other primes as it is the only exceptional case. This section is dedicated to the treatment of Schur rings over Z_{2^n}.

As in the odd case, we mention that the notation introduced in Definition 5.1 applies for $p = 2$ also. There are two critical differences between $\mathcal{L}_{2^n}$ and $\mathcal{L}_{p^n}$, for p odd, that should be mentioned. First, there is no first layer on $\mathcal{L}_{2^n}$ since $\mathcal{L}_2 = \mathcal{L}_1 = \{\mathbb{Q}\}$. This will cause our recurrence relation on $\Omega(n)$ to have "extra" initial conditions, that is, the recursion does not stabilize until the fourth stage, as opposed to the second stage for odd primes. Second, the Galois group of $\mathcal{K}_{2^n}$ is not cyclic for $n \geq 3$. This gives the lattice $\mathcal{L}_{2^n}$ a different shape than the other lattices we have seen, which translates to different recurrence relations on $\Omega(n,k)$, which we will see below.

Despite these differences, there are still some important similarities between the even and odd cases. For example, it still holds that $\Omega(0) = 1$. Another similarity is the fact that $\Omega(1) = 1$, which is the number of divisors of $2 - 1 = 1$. It also holds that Proposition 5.2, Proposition 5.4, and Proposition 5.5 (for all $n \geq 3$ and $2 < k \leq n$) remain true if $p = 2$ by the same proofs as before. From these, we can compute

$$\Omega(2) = \Omega(2,0) + \Omega(2,2) = (\Omega(0) + \Omega(1)) + 1 = 3.$$

Now, Proposition 5.3 no longer applies since there is no first layer. Instead, we will treat $k = 2$ as the base case in the recurrence relation on $\Omega(n,k)$.

Proposition 6.1. *For $n \geq 3$, the number of Schur rings over Z_{2^n} mapping to $\mathcal{K}_4 = \mathbb{Q}(i)$ with respect to ω is equal to the difference between number of Schur rings over $Z_{2^{n-1}}$ and the number of Schur rings over $Z_{2^{n-2}}$ mapping onto $\mathbb{Q}$, that is,*

$$\Omega(n,2) = \Omega(n-1) - \Omega(n-2,0). \tag{6.1}$$

When $n = 2$, we have $\Omega(2, 2) = 1$ by (5.3).

Proof. Let S be a Schur ring over Z_{2^n} such that $\omega(S) = \mathbb{Q}(i)$. Since $n \geq 3$, it must be that S is wedge-decomposable of the form $S = \mathbb{Q}[Z_4] \wedge T$ for some Schur ring T over $Z_{2^{n-1}}$ such that $T \cap \mathbb{Q}[Z_2] = \mathbb{Q}[Z_2]$, by the same reasoning used in Proposition 5.5. Now, every Schur ring over $Z_{2^{n-1}}$ has this property except those of the form $T = \mathbb{Q}[Z_{2^k}]^0 \wr T'$ for $1 < k \leq n-1$. Now, there are exactly $\Omega(n-2, 0)$ such Schur rings by Proposition 5.2. Therefore, the result follows. □

The major consequence of $\mathcal{G}_{2^n}$ not being cyclic is that Proposition 5.6 fails for some of the layers of $\mathcal{L}_{2^n}$. For example, the number of Schur rings over Z_{16} which map onto $\mathcal{K}_8 = \mathbb{Q}(\zeta_8)$ is three but the number of Schur rings mapping onto $\mathbb{Q}(\zeta_8 + \zeta_8^{-1})$ is four. By Section 2, for $k \geq 3$, the kth layer of $\mathcal{L}_{2^n}$ contains three fields: $\mathbb{Q}(\zeta_{2^k})$, $\mathbb{Q}(\zeta_{2^k} + \zeta_{2^k}^{-1})$, and $\mathbb{Q}(\zeta_{2^k} - \zeta_{2^k}^{-1})$. Let $\Omega_{\mathcal{S}}(n, k)$ be the number of Schur rings over Z_{2^n} which map onto $\mathbb{Q}(\zeta_{2^n} + \zeta_{2^n}^{-1})$ via ω. It holds that $\mathcal{S}(Z_{2^n})$ is the unique Schur ring over Z_{2^n} which maps onto $\mathbb{Q}(\zeta_{2^n} + \zeta_{2^n}^{-1})$, by Theorem 4.9. This gives the following formula:

$$\Omega_{\mathcal{S}}(n, n) = 1. \tag{6.2}$$

Likewise, $\mathbb{Q}[Z_{2^n}]^{\langle \sigma_{2^{n-1}-1} \rangle}$ is the unique Schur ring over Z_{2^n} which maps onto $\mathbb{Q}(\zeta_{2^n} - \zeta_{2^n}^{-1})$. So for the top layer, the number of Schur rings mapping onto a given field is constant. This fact allows use to compute $\Omega(3)$:

$$\Omega(3) = \Omega(3, 0) + \Omega(3, 2) + 3\Omega(3, 3) = (\Omega(0) + \Omega(1) + \Omega(2)) + (\Omega(2) - \Omega(0)) + 3 = 10.$$

Although Proposition 5.6 is false in general for $p = 2$, it is still "mostly" true, as explained in the next proposition.

Proposition 6.2. *The number of Schur rings over Z_{2^n} mapping onto $\mathbb{Q}(\zeta_{2^k} + \zeta_{2^k}^{-1})$ via ω is the same as the number of Schur rings mapping onto $\mathbb{Q}(\zeta_{2^k} - \zeta_{2^k}^{-1})$.*

Proof. If $\mathbb{Q}(\zeta_{2^k} + \zeta_{2^k}^{-1})$ and $\mathbb{Q}(\zeta_{2^k} - \zeta_{2^k}^{-1})$ are in the top layer, then there is exactly one Schur ring mapping onto each field by (6.2). Otherwise, each Schur ring mapping onto these fields must be wedge-decomposable. Let $\pi : Z_{2^n} \to Z_{2^{n-1}}$ be the natural quotient map. Then $\pi(\mathcal{S}(Z_{2^k})) = \pi(\mathbb{Q}[Z_{2^k}]^{\langle \sigma_{2^k-1} \rangle}) = \mathcal{S}(Z_{2^{k-1}}) = \pi(\mathbb{Q}[Z_{2^k}]^{\langle \sigma_{2^{k-1}-1} \rangle})$. Since the images are the same, the number of possible wedge products which map on $\mathbb{Q}(\zeta_{2^k} + \zeta_{2^k}^{-1})$ is the same as the number of possible wedge products which map onto $\mathbb{Q}(\zeta_{2^k} - \zeta_{2^k}^{-1})$. □

Theorem 6.3. *The number of Schur rings over Z_{2^n}, where $n \geq 3$, is given by the following equation:*

$$\Omega(n) = \Omega(n,0) + \Omega(n,2) + \sum_{k=3}^{n} (\Omega(n,k) + 2\Omega_{\mathcal{S}}(n,k)). \tag{6.3}$$

Proof. There is exactly one field in the 0th layer and the second layer of $\mathcal{L}_{2^n}$. Each other layer of $\mathcal{L}_{2^n}$ contains three fields: $\mathbb{Q}(\zeta_{2^n})$, $\mathbb{Q}(\zeta_{2^n} + \zeta_{2^n}^{-1})$, and $\mathbb{Q}(\zeta_{2^n} - \zeta_{2^n}^{-1})$. The equation then follows from Proposition 6.2. □

A direct consequence of (6.3) and Lemma 5.10 is the following:

$$\Omega(n) = \Omega(n,0) + \sum_{k=0}^{n-2} c_k \Omega(n-k,2) + 2\sum_{k=3}^{n} \Omega_{\mathcal{S}}(n,k) \tag{6.4}$$

Therefore, we seek to express $2\sum_{k=3}^{n} \Omega_{\mathcal{S}}(n,k)$ in terms of the $\Omega(n,k)$.

Proposition 6.4. *For $k > 3$,*

$$\Omega_{\mathcal{S}}(n,k) = \Omega_{\mathcal{S}}(n-1,k-1) + 2\sum_{j=k}^{n-1} \Omega_{\mathcal{S}}(n-1,j) \tag{6.5}$$

Proof. Following the same reasoning as (5.4), we see (6.5) is true for $k = n$ by (6.2) and for $k < n$, it suffices to count the number of Schur rings T over $Z_{2^{n-1}}$ for which $T \cap \mathbb{Q}[Z_{2^{k-1}}] = \mathcal{S}(Z_{2^{k-1}})$. This is exactly the number of Schur rings over $Z_{2^{n-1}}$ which map onto $\mathbb{Q}(\zeta_{2^j} + \zeta_{2^j}^{-1})$ for $k-1 \leq j \leq n-1$ or onto $\mathbb{Q}(\zeta_{2^j} - \zeta_{2^j}^{-1})$ for $k-1 < j \leq n-1$. The result then follows from Proposition 6.2. □

Proposition 6.5. *For $n > 3$,*

$$\Omega_{\mathcal{S}}(n,3) = \Omega(n-1,2) + 2\sum_{j=3}^{n-1} \Omega_{\mathcal{S}}(n-1,j) \tag{6.6}$$

Proof. Following the same reasoning as (5.4), it suffices to count the number of Schur rings T over $Z_{2^{n-1}}$ for which $T \cap \mathbb{Q}[Z_4] = \mathbb{Q}[Z_2] \wr \mathbb{Q}[Z_2]$. This includes the Schur rings over $Z_{2^{n-1}}$ which map onto $\mathbb{Q}(\zeta_{2^j} + \zeta_{2^j}^{-1})$ for $3 \leq j \leq n-1$ or onto $\mathbb{Q}(\zeta_{2^j} - \zeta_{2^j}^{-1})$ for $3 \leq j \leq n-1$. On the other hand, no Schur ring which maps onto $\mathbb{Q}(\zeta_{2^j})$ has this property for $j > 1$. It remains to examine which Schur rings that map onto $\mathbb{Q}$ have this property. By Theorem 4.7, any Schur ring over $Z_{2^{n-1}}$ mapping onto $\mathbb{Q}$ has the form $T = \mathbb{Q}[Z_2] \wr T'$ for some Schur ring T' over $Z_{2^{n-2}}$ such that $T' \cap \mathbb{Q}[Z_2] = \mathbb{Q}[Z_2]$, since $T \cap \mathbb{Q}[Z_4] = \mathbb{Q}[Z_2] \wr \mathbb{Q}[Z_2]$. As was seen in the proof of Proposition 6.1, the number of choices for T' is $\Omega(n-1,2)$. The result then follows from Proposition 6.2. □

Next, we need to expand $2\sum_{k=3}^{n}\Omega_{\mathcal{S}}(n,k)$ using (6.5) and (6.6). This will produce an equation of the following form:

$$2\sum_{k=3}^{n}\Omega_{\mathcal{S}}(n,k)=\sum_{i=1}^{n-2}s_i\Omega(n-i,2) \tag{6.7}$$

for some positive integers s_i. In particular, the jth iteration of (6.5) and (6.6) will produce an equation of the form

$$2\sum_{k=3}^{n}\Omega_{\mathcal{S}}(n,k)=\sum_{i=1}^{j-1}s_i\Omega(n-i,2)+\sum_{k=j+1}^{n}s_{jk}\Omega_{\mathcal{S}}(n-j,k-j) \tag{6.8}$$

for some positive integers s_{jk}. We note that $s_{i(i+1)}=s_i$ and $s_{0k}=1$ for all k. Furthermore,

$$s_{jk}=s_{(j-1)k}+2\sum_{\ell=j}^{k-1}s_{(j-1)\ell} \tag{6.9}$$

by (6.5). When $0<j<k-1$, (6.9) can be rewritten recursively to give

$$s_{jk}=s_{(j-1)k}+s_{j(k-1)}+s_{(j-1)(k-1)}. \tag{6.10}$$

From (6.10), we can create a triangular array of integers, depicted in Figure 8, where k indexes the rows ($k\geq 1$) and j indexes the columns ($0\leq j<k$). The diagonal entries of the triangle give the values of s_i.

FIGURE 8. The Triangular Array of s_{jk} Coefficients

1							
1	3						
1	5	11					
1	7	23	45				
1	9	39	107	197			
1	11	59	205	509	903		
1	13	83	347	1061	2473	4279	
1	15	111	541	1949	5483	12235	20793

Lemma 6.6. *Let s_i be the coefficients given in Equation (6.7). Then $s_i = \sum_{j=0}^{i} \frac{1}{j+1}\binom{2j}{2}\binom{i+j}{2j}$, that is, s_i is the ith Schröder number.*

Proof. Like in Lemma 6.6, we define $s_{00} = 1$ and $s_{jj} = s_{(j-1)j}$ for $j > 0$. Now, this new triangular array is known as the Super-Catalan Triangle. One property of this triangle is that the sequence of diagonal entries is the sequence of super-Catalan numbers, also known as the little Schröder numbers [4]. Multiplying the little Schröder numbers by two and reindexing gives the Schröder numbers. □

Theorem 6.7. *The number of Schur rings over Z_{2^n}, where $n \geq 2$, is given by the following recursive equation:*

$$\Omega(n) = \sum_{k=1}^{3} 2^k \Omega(n-k) - (c_{n-1} + s_{n-1}) + \sum_{k=4}^{n} \left(c_{k-1} + s_{k-1} - \sum_{j=1}^{k-3} (c_j + s_j) \right) \Omega(n-k) \tag{6.11}$$

where $\Omega(0) = 1$, $\Omega(1) = 1$, $\Omega(2) = 3$, $\Omega(3) = 10$, $c_k = \dfrac{1}{k+1}\binom{2k}{k}$ is the kth Catalan number, and $s_k = \sum_{j=0}^{k} \frac{1}{j+1}\binom{2j}{2}\binom{k+j}{2j}$ is the kth Schröder number.

For $n < 4$, we consider the second sum in (6.11) to be empty. Also, we define $\Omega(-1) = 0$, which appear in (6.11) for $n = 2$.

Proof. By (6.4),

$$\Omega(n) = \Omega(n,0) + \sum_{k=0}^{n-2} c_k \Omega(n-k,2) + 2\sum_{k=3}^{n} \Omega_{\mathcal{S}}(n,k),$$

which by Lemma 6.6, can be rewritten as

$$\begin{aligned}
\Omega(n) &= \Omega(n,0) + \sum_{k=0}^{n-2} c_k \Omega(n-k,2) + \sum_{k=1}^{n-2} s_k \Omega(n-k,2) \\
&= \Omega(n,0) + \Omega(n,2) + \sum_{k=1}^{n-2} (c_k + s_k)\Omega(n-k,2) \\
&= \Omega(n,0) + \Omega(n,2) + (c_{n-2} + s_{n-2}) + \sum_{k=1}^{n-3} (c_k + s_k)\Omega(n-k,2).
\end{aligned}$$

We next can apply Proposition 6.1 to the above equation:

$$\begin{aligned}
\Omega(n) &= \Omega(n,0) + [\Omega(n-1) - \Omega(n-2,0)] + (c_{n-2} + s_{n-2}) \\
&\qquad + \sum_{k=1}^{n-3} (c_k + s_k)[\Omega(n-k-1) - \Omega(n-k-2,0)] \\
&= \Omega(n-1) + \sum_{k=1}^{n-3} (c_k + s_k)\Omega(n-k-1) + (c_{n-2} + s_{n-2}) + \Omega(n,0)
\end{aligned}$$

$$\begin{aligned}
& -\Omega(n-2,0) - \sum_{k=1}^{n-3}(c_k+s_k)\Omega(n-k-2,0) \\
= \quad & \Omega(n-1) + \sum_{k=2}^{n-2}(c_{k-1}+s_{k-1})\Omega(n-k) + (c_{n-2}+s_{n-2}) + \Omega(n,0) \\
& -\Omega(n-2,0) - \sum_{k=3}^{n-1}(c_{k-2}+s_{k-2})\Omega(n-k,0) \\
= \quad & \Omega(n-1) + \sum_{k=2}^{n-1}(c_{k-1}+s_{k-1})\Omega(n-k) + \Omega(n,0) - \Omega(n-2,0) \\
& - \sum_{k=3}^{n-1}(c_{k-2}+s_{k-2})\Omega(n-k,0).
\end{aligned}$$

Next we apply Proposition 5.2 to the above equation:

$$\Omega(n) = 2\Omega(n-1) + \Omega(n-2) + \sum_{k=2}^{n-1}(c_{k-1}+s_{k-1})\Omega(n-k) - \sum_{k=3}^{n-1}(c_{k-2}+s_{k-2})\sum_{j=0}^{n-k-1}\Omega(j).$$

We note that

$$\begin{aligned}
\sum_{k=3}^{n-1}(c_{k-2}+s_{k-2})\sum_{j=0}^{n-k-1}\Omega(j) &= \sum_{k=3}^{n-1}\sum_{j=0}^{n-k-1}(c_{k-2}+s_{k-2})\Omega(j) = \sum_{j=0}^{n-4}\sum_{k=3}^{n-j-1}(c_{k-2}+s_{k-2})\Omega(j) \\
&= \sum_{k=0}^{n-4}\sum_{j=3}^{n-k-1}(c_{j-2}+s_{j-2})\Omega(k) = \sum_{k=4}^{n}\sum_{j=3}^{k-1}(c_{j-2}+s_{j-2})\Omega(n-k).
\end{aligned}$$

Therefore,

$$\begin{aligned}
\Omega(n) &= 2\Omega(n-1) + \Omega(n-2) + \sum_{k=2}^{n-1}(c_{k-1}+s_{k-1})\Omega(n-k) - \sum_{k=4}^{n}\sum_{j=3}^{k-1}(c_{j-2}+s_{j-2})\Omega(n-k) \\
&= 2\Omega(n-1) + 4\Omega(n-2) + 8\Omega(n-3) - (c_{n-1}+s_{n-1}) \\
&\qquad + \sum_{k=2}^{n-1}\left(c_{k-1}+s_{k-1} - \sum_{j=3}^{k-1}(c_{j-2}+s_{j-2})\right)\Omega(n-k) \\
&= \sum_{k=1}^{3}2^k\Omega(n-k) - (c_{n-1}+s_{n-1}) + \sum_{k=4}^{n}\left(c_{k-1}+s_{k-1} - \sum_{j=1}^{k-3}(c_j+s_j)\right)\Omega(n-k). \quad \square
\end{aligned}$$

Table 6.1 lists the number of Schur rings over Z_{2^n} up to the tenth power.

Let $\mathcal{F}(z) = \sum_{n=0}^{\infty}\Omega(n)z^n$ be the generating function of Ω, for $p = 2$. Using

$$\mathcal{C}(z) = \sum_{n=0}^{\infty}c_n z^n = \frac{1-\sqrt{1-4z}}{2z},$$

TABLE 6.1. Number of Schur Rings over Z_{2^n}

n	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
$\Omega(n)$	1	3	10	37	151	657	2,989	14,044	67,626	332,061

the generating function for the Catalan numbers,

$$\mathcal{S}(z) = \sum_{n=0}^{\infty} s_n z^n = \frac{1 - z - \sqrt{1 - 6z + z^2}}{2z},$$

be the generating function for the Schröder numbers, and the usual generating function calculations, one computes that

$$\mathcal{F}(z) = \frac{(2 - z - \sqrt{1-4z} - \sqrt{1-6z+z^2})(1-z) + 2(z^2-1)}{(2 - z - \sqrt{1-4z} - \sqrt{1-6z+z^2})(1-z-z^2) + 2(z^3+z^2+z-1)}. \tag{6.12}$$

Acknowledgments: The contents of this paper are part of the author's doctoral dissertation [15], written under the supervision of Stephen P. Humphries, that was submitted to Brigham Young University. All computations made in preparation of this paper were accomplished using the computer software Magma [1] and the exact code can be found in [15] and [7], the second reference being the master's thesis of Brent Kerby, another student of Humphries. Helpful suggestions, instructions, and guidance were offered to the author by Michael Barrus on many of combinatorical topics in this paper. Finally, acknowledgment should be given by Petr Vojtechovsky for his insights on how the topics of this paper related to the PORC conjecture.

REFERENCES

[1] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[2] Marcus du Sautoy and M.R. Vaughan-Lee. Non-porc behaviour of a class of descendant p-groups. *Journal of Algebra*, 361:287–312, 2012.

[3] Anton Evseev. Higman's porc conjecture for a family of groups. *Bulletin of the London Mathematical Society*, 40(3):415–431, 2008.

[4] Johannes Fischer. Sequence a144944. *The On-Line Encyclopedia of Integer Sequences*.

[5] G. Higman. Enumerating p-groups. i: Inequalities. *Proceedings of the London Mathematical Society*, 10(3):24–30, 1960.

[6] G. Higman. Enumerating p-groups. ii: Problems whose solution is porc. *Proceedings of the London Mathematical Society*, 10(3):566–582, 1960.

[7] Brent Kerby. Rational schur rings over abelian groups. Master's thesis, Brigham Young University, 2008.

[8] M. Kh. Klin and R. Poschel. The konig problem, the isomorphism problem for cyclic graphs and the method of schur rings. *Algebraic Methods in Graph Theory*, 1, 2, 1978.

[9] István Kovács. The number of indecomposable schur rings over a cyclic 2-group. *Séminaire Lotharingien de Combinatoire*, 51:Article B51h, 2005.

[10] Ka Hin Leung and Siu Lun Ma. The structure of schur rings over cyclic groups. *Journal of Pure and Applied Algebra*, 66:287–302, 1990.

[11] Ka Hin Leung and Shin Hing Man. On schur rings over cyclic groups ii. *Journal of Algebra*, 183:273–285, 1996.

[12] Ka Hin Leung and Shin Hing Man. On schur rings over cyclic groups. *Israel Journal of Mathematics*, 106:251–267, 1998.

[13] V. Liskovets and R. Poschel. Counting circulant graphs of prime-power order by decomposing into orbit enumeration problems. *Discr. Math.*, 214:173–191, 2000.

[14] S. L. Ma. On association schemes, schur rings, strongly regular graphs and partial difference sets. *Ars Combin.*, 21:211–220, 1989.

[15] Andrew Misseldine. *Algebraic and Combinatorial Properties of Schur Rings over Cyclic Groups*. PhD thesis, Brigham Young University, 2014.

[16] Mikhail Muzychuk. The structure of schur rings over cyclic groups of square-free order. *Acta Applicandae Mathematicae*, 52:163–181, 1998.

[17] Mikhail E. Muzychuk. The structure of rational schur rings over cyclic groups. *European Journal of Combinatorics*, 14:479–490, 1993.

[18] Mikhail E. Muzychuk. On the structure of basic sets of schur rings over cyclic groups. *Journal of Algebra*, 169:655–678, 1994.

[19] M.F. Newman, E.A. O'Brien, and M.R. Vaughan-Lee. Groups and nilpotent lie rings whose order is the sixth power of a prime. *Journal of Algebra*, 278(1):383–401, 2004.

[20] E.A. O'Brien and M.R. Vaughan-Lee. The groups with order p^7 for odd prime p. *Journal of Algebra*, 292(1):243–258, 2005.

[21] N. J. A. Sloane. Sequence a009766. *The On-Line Encyclopedia of Integer Sequences*.

[22] Helmut Wielandt. Zur theorie der einfach transitiven permutationsgruppen II (German). *Math. Z.*, 52:384–393, 1949.

[23] Helmut Wielandt. *Finite Permutation Groups*. Academic Press, New York-London, 1964.

[24] Brett E. Witty. Enumeration of groups of prime-power order. *Bulletin of the Australian Mathematical Society*, 76:479–480, 12 2007.